Journal of Korea Multimedia Society Vol. 7, No. 7, July 2004(pp. 913-921)

카툰 화상을 이용한 심층암호에 관한 연구

박영란[†], 박지환[††]

요 약

데이터 은닉(data hiding)의 한 분야인 심층암호(steganography)는 제3자가 기밀정보의 삽입여부를 인지하지 못하도록 디지털화된 각종 미디어에 몰래 숨겨서 송/수신자간에 비밀통신을 할 수 있는 방법이다. 그러나 흑백으로만 구성되는 스캔된 텍스트 화상나 카툰 화상 등에 시각적으로 인지되지 않도록 기밀정보를 숨기는 것은 쉽지 않다. 본 논문에서는 이진 카툰 화상을 3×3 크기의 블록으로 분할한 후, 그 블록의 가운데 픽셀을 둘러싼 8-이웃 픽셀의 연속 길이를 이용하여 기밀 데이터를 숨기는 방식을 제안한다. 제안 방식은 어떤 조건에서는 가운데 픽셀에도 데이터를 은닉시켜 기밀정보의 삽입량을 증가시킬 수 있음을 보인다.

A Study on Steganography Using Cartoon Image

Young-Ran Park[†], Ji-Hwan Park[††]

ABSTRACT

Steganography is a kind of data hiding which can hide secret information to digital media. It is performed so that another person does not recognize any information and make secret communication between each other. Specially, it is not easy to hide secret information without being visually recognized in scanned text image or cartoon image etc. In this paper, we propose an improved method that can embed a large quantity of secret information in a binary image without noticeable artifacts. Binary cartoon image is divided into block of 3-by-3 sizes. Secret information is embedded by using run-length of 8-neighborhood pixels except for the center pixel of the block. To improve the embedding capacity, we embed it into center pixel under to some condition.

Key words: Information Hiding(정보은닉), Steganography(심층암호), Binary Image, Watermarking

1. 서 론

컴퓨터 산업의 성장과 함께 인터넷의 보급이 급속도로 발달함에 따라 다양한 디지털 미디어들이 폭넓은 인기를 모으면서 정보의 교환이 활발해지고 있다. 이러한 디지털 미디어들의 장점은 편리하게 전송 가능하며, 쉽게 접근 및 편집이 가능하고, 손실 없이 복사할 수 있다는 것이다. 그러나 이러한 장점에도 불구하고 보안에 관한 많은 문제가 대두되고 있으며, 최근 이러한 문제를 해결하기 위한 방법으로 데이터 은닉(data hiding) 기술에 관한 연구가 주목을 받고 있다[1,2]. 데이터 은닉 기술은 크게 저작권 보호가 목적인 디지털 워터마킹(digital watermarking) 기술, 부정자 추적 기능이 추가된 핑거프린팅(fingerprinting) 기술과 비밀통신이 목적인 심층암호(steganography)로 분류된다.

디지털 워터마킹은 디지털 컨텐츠의 소유자 정보인 워터마크를 컨텐츠 내부에 어떤 형태로 삽입을 시켜놓고 저작권 문제가 발생했을 때, 해당 컨텐츠에서 워터마크를 추출함으로써 원 소유자의 저작권을

※ 교신저자(Corresponding Author) : 박영란, 주소 : 부산시 남구 대연3동 599-1, 전화 : 051)620-6392, FAX : 051)620-6390, E-mail : podosongei@hanmail.net
접수일 : 2003년 8월 29일, 완료일 : 2003년 12월 10일
[†]준회원, 부경대학교 대학원 정보보호학과 박사과정
[††]종신회원, 부경대학교 전자컴퓨터정보통신공학부 교수
(E-mail : jpark@pknu.ac.kr)
※ 이 논문은 2001학년도 부경대학교발전기금의 지원에 의하여 연구되었음.

주장할 수 있는 저작권 보호 기술이다. 이때 워터마크의 양은 다소 무관하며, 추출 역시 완벽하게 추출되지 않고 특정 기준 값 이상이면 저작권을 인정하기도 한다. 이러한 워터마킹 기술은 워터마크를 어떤 영역에서 삽입하느냐에 따라 공간 영역 워터마킹(spatial domain watermarking)과 주파수 영역 워터마킹(frequency domain watermarking)으로 분류할 수 있다.

디지털 핑거프린팅(digital fingerprinting) 기술은 디지털 워터마킹과 유사한 기술이나, 차이점은 컨텐츠에 삽입되는 워터마크(watermark)로 컨텐츠를 구매하려는 구매자의 정보를 삽입하는 것이다. 따라서 불법 배포 및 재분배를 방지하기 위한 부정자 추적의 기능으로 이용할 수 있다.

한편, 심층암호(steganography)는 암호기술의 한 방법으로써, 화상에 적용한 것을 화상 심층암호(image steganography)라 한다. 대부분의 화상 심층암호에서는 시각적인 손상을 줄이기 위해 컬러 화상 또는 그레이(gray scale) 화상을 이용하여 기밀 데이터를 은닉하는 경우가 많다. 그러나 일반적으로 인터넷상에 전송되는 데이터들은 두 값으로만 구성된 이진 화상도 널리 이용되고 있으므로 본 논문에서는 이진 카툰 화상(binary cartoon image)에 기밀 데이터를 은닉하는 방법을 제안한다.

본 논문에서 제안하는 방식은 이진 카툰 화상을 동일한 크기의 여러 블록으로 나누고, 대상 블록의 가운데 픽셀을 기준으로 하여 그 주변을 둘러싼 이웃 화소들의 상태에 따라 데이터를 은닉한다. 기존의 방식보다 시각적으로 영향을 적게 주면서 은닉 데이터의 양이 많다는 것을 실험을 통하여 확인할 수 있었다.

본 논문의 2장에서는 기존의 관련 연구들[3,4]을 분석하고, 3장에서는 제안 방식에 대해서 기술한다. 4장에서는 실험을 통하여 기존 방식과 제안 방식을 비교를 하며, 마지막 5장에서는 결론을 제시한다.

2. 관련 연구

최근, 이진 화상에 기밀 정보를 은닉하는 많은 방법들이 연구되어져 왔다[2-5,7-10]. 본 장에서는 이러한 기존 연구들 중에서 이진 카툰 화상에 기밀 정보를 은닉하는 방식 중에서 대표적인 WL 방식[3]과 PWW 방식[4]에 대하여 살펴본다.

2.1 WL 방식

이 방식은 호스트 이진 화상 F를 $m \times n$ 크기의 블록 F_i로 분할시킨 후, F_i가 삽입 가능한 블록인지 아닌지를 식(1)을 이용하여 판단한다.

$$0 < SUM(F_i \,\&\, K) < SUM(K) \qquad (1)$$

여기서 &은 AND 논리 연산자이며, SUM은 요소들의 합을 의미하지만 호스트 화상이 이진 화상이므로 화소 값이 0 또는 1(흑/백)의 값을 가진다. 따라서 블록 내에 1의 값을 가지는 요소의 개수라 할 수 있다. 그리고 K는 F_i와 동일한 크기의 비밀 키 블록이다. 기밀 정보의 삽입은 대상 블록이 식(1)에 따라 조건을 만족하는 블록에 대해서만 다음의 삽입 알고리즘에 의해서 기밀 정보를 숨기며, 그렇지 않으면 제외시키는 방식이다. 이런 과정을 전체 블록에 대해서 반복 처리를 수행한다.

예를 들어, 삽입할 기밀 데이터 비트열이 "0 1 1"이라 가정했을 때, 삽입 알고리즘에 의해 그림 1과 같은 삽입 결과를 얻을 수 있다. 즉, 삽입 알고리즘은 $SUM(F_i \,\&\, K) \bmod 2$를 계산한 값이 b와 같은 경우는 픽셀 값을 변경하지 않으며, 그렇지 않은 경우에 대해서는 어떤 한 픽셀을 변경해야 한다. 변경을 할 때에는 우선, $[K]_{j,k} = 1$ 인 것과 대응되는 $[F_i]_{j,k}$의 픽셀 값을 0이면 1로 변경하고, 1이면 0으로 변경을 하면 된다. 또한 이 알고리즘에서는 예외처리가 존재한다. 즉, $SUM(F_i \,\&\, K) = 1$ 과 $SUM(F_i \,\&\, K) = SUM(K) - 1$ 인 경우이다. 전자의 경우는 블록에서

〈WL 방식의 삽입 알고리즘〉

```
if (SUM(F_i & K) mod 2 = b) then  불변경
else if (SUM(F_i & K) = 1) then
        [K]_{j,k} = 1 AND [F_i]_{j,k} = 0 인 픽셀을
        [F_i]_{j,k} = 1 로 변경
else if (SUM(F_i & K) = (SUM(K) - 1) then
        [K]_{j,k} = 1 AND [F_i]_{j,k} = 1 인 픽셀을
        [F_i]_{j,k} = 0 으로 변경
else
   [K]_{j,k} = 1 인 [F_i]_{j,k}의 픽셀 값을
            0은 1로, 1은 0으로 변경
end if;
```

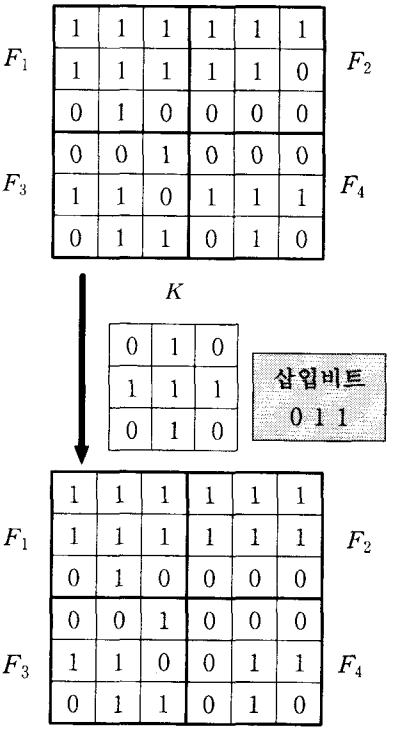


그림 1. WL 방식의 삽입 예

1인 픽셀 값을 0으로 변경을 하게 되면, 기밀 데이터 추출할 때 식(1)의 조건에 만족을 하지 않기 때문에 그 블록은 기밀 데이터가 삽입한 블록인데도 불구하고 추출을 못하게 되므로 블록 F_i에서 0인 픽셀 값이 1이 되도록 조절을 한다. 후자의 경우에도 추출할 경우 식(1)에 만족이 되도록 하기 위해 블록 F_i에 1인 픽셀 값이 0이 되도록 조절을 한다.

기밀 데이터 추출은 식(1)을 만족하는 블록에 대해서 $SUM(F_i \& K) \equiv b \pmod 2$인 b를 추출해 낼 수 있다.

2.2 PWW 방식

이 방식의 기본 개념은 화상의 한 픽셀은 그 주변의 픽셀들과 강한 의존성을 가진다는 성질을 이용하는 것이다. 그러므로 데이터를 은닉시키기 위해서 어떤 주목 픽셀을 변경해야 한다면 그 주변을 둘러싼 이웃 픽셀들과의 의존 상태에 따라 우선순위를 부여한다. 그리고 기밀 데이터를 삽입시킬 때는 우선순위가 높은 블록에 대해서 먼저 삽입을 시키는 방식이다. 예를 들어, 그림 2(a)의 패턴과 그림 2(b)의 패턴

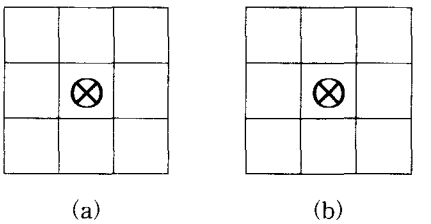


그림 2. 다른 순위를 가지는 3×3 블록의 두 패턴

을 가진 두 블록에서 각각의 가운데 픽셀을 변경시킨다고 가정하면 그림 2(a)는 시각적으로 바로 감지가 되겠지만, 그림 2(b)는 그다지 눈에 띄지 않을 것이다. 그러므로 그림 2(a)의 패턴 보다 그림 2(b)의 패턴이 더 높은 우선순위를 가지게 된다[4,6].

삽입 방법은 호스트 이진 화상을 여러 블록으로 분할한 후, 각 블록의 패턴 모양에 따라 우선순위를 부여하기 위해 분류를 한다.

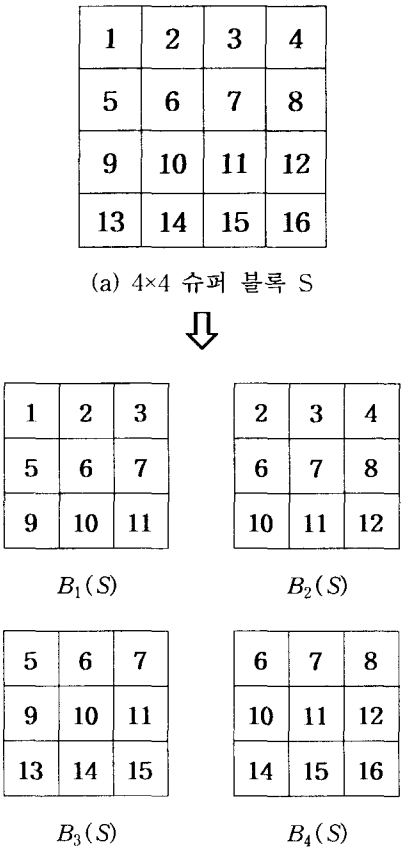
그런 다음 우선 순위가 가장 높은 블록들에 대해서 기밀 데이터 1비트를 먼저 삽입시키고, 기밀 데이터가 모두 삽입되지 않고 남아 있을 경우는 그 다음 우선순위를 가진 블록으로 계속 진행해 나간다. 삽입 원리는 블록의 가운데 픽셀의 값을 식(2) 또는 식(3)과 같이 변경을 시키는데, 기밀성의 측면에서는 식(2) 보다 식(3)이 비밀 키 테이블 K를 이용하였기 때문에 더욱 안전하다고 볼 수 있다.

$$c = h \tag{2}$$

$$c = (SUM(B \oplus K) + h) \mod 2 \tag{3}$$

여기서 c는 가운데 픽셀이며, h는 기밀 데이터 비트이고, B는 블록, K는 비밀 키 테이블을 의미한다. 또한, PWW 방식에서는 삽입량과 화질을 개선하기 위해서 슈퍼 블록(super block)이라는 개념을 도입하였다. 예를 들면, 그림 3(a)와 같이 4×4 크기의 슈퍼 블록 S 안에는 그림 3(b)와 같이 4개의 3×3 크기의 서브 블록 B를 가질 수 있다. 따라서 4개의 서브 블록 $B_i(S)$ $(i=1,2,3,4)$ 중에서도 가장 높은 순위를 가지는 서브 블록의 가운데 픽셀을 변경시키는 방법이다. 즉, 그림 3(b)에서는 $B_3(S)$ 인 서브 블록의 가운데 픽셀을 변경시킨다. 추출은 송/수신자가 공유하고 있는 K와 우선순위를 이용하여 삽입과정과 동일하게 수행하여 이루어지게 된다.

위에서 소개한 WL 방식은 기밀 데이터 삽입량은 비밀 키 블록을 구성하는 요소 값에 따라 약간의 차



(a) 4×4 슈퍼 블록 S

$B_1(S)$ $B_2(S)$

$B_3(S)$ $B_4(S)$

(b) 3×3 서브 블록 B

그림 3. 슈퍼 블록 방식

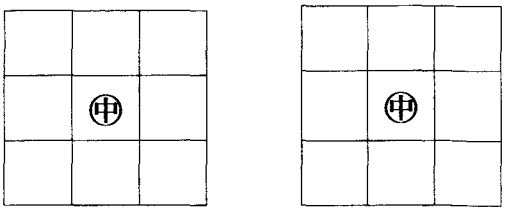
이는 있겠지만, 화질을 어느 정도 고려한다면 블록 내의 0과 1의 개수가 비슷해야 할 것이다. 따라서 식 (1)의 조건을 만족하는 블록에만 기밀 데이터가 삽입되므로 삽입량이 그다지 많지 않고, 더욱이 특정 픽셀을 변경시킬 때 그 이웃 픽셀의 상태를 전혀 고려하지 않았기 때문에 카툰 화상의 윤곽부분 주위에서 약간 벗어난 부분에 잡음들이 존재하여 화질이 떨어지는 문제점이 있다. 한편, PWW 방식에서는 높은 우선순위를 가진 블록에만 기밀 데이터를 삽입한다면 화질은 우수하나, 전송하고자 하는 기밀 데이터의 양을 증가시키면 우선순위가 낮은 블록에도 삽입을 시켜야 되기 때문에 화질의 열화가 많이 발생하게 된다. 그러므로 삽입할 기밀 데이터의 양이 많을 경우 적합하지 않는 문제점이 있다. 따라서 이러한 취약점들을 보완할 수 있는 간단하면서도 삽입량과 화질 면에서 우수한 알고리즘을 다음 장에서 제안한다.

3. 제안 방식

3.1 8-이웃 픽셀 적용

제안 방식은 이진 화상의 어떤 블록 내의 한 픽셀은 그 이웃 픽셀과 강한 의존성을 가진다는 사실에 기반 하였다[4,6]. 화상의 한 픽셀을 중심으로 해서 사방으로 둘러싼 픽셀들을 이웃 픽셀이라고 한다. 이웃 픽셀이라 함은 그림 4와 같이 4-이웃 픽셀들과 8-이웃 픽셀들이 있다. 특히, 이진 화상의 픽셀 값은 0 또는 1의 값을 가지므로 중심에 위치한 가운데(핵) 픽셀 값과 이웃 픽셀들의 값은 서로 상관을 가진다. 따라서 본 논문에서는 이진 화상을 여러 블록으로 분할하고, 블록의 패턴에 대해서 가운데 픽셀과 이웃 픽셀들의 상호 의존성을 이용하여 기밀 데이터를 삽입하는 방법을 제안한다.

기밀 데이터의 삽입은 이진 카툰 화상 H를 3×3 블록으로 분할하고, 그 블록 h의 가운데 픽셀을 중심으로 8-이웃 픽셀들의 연속 길이(run-length)를 짝수 혹은 홀수로 조절하여 기밀 데이터인 0 또는 1을 삽입한다. 여기서 연속 길이(run-length)라는 것은 8-이웃 픽셀들을 1차원적으로 나열을 했을 때, 픽셀 값이 특정 위치에서부터 시작하여 연속적으로 동일한 값을 가지는 길이를 말한다. 제안 방식에서는 그림 5와 같이 8-이웃 픽셀의 연속 길이가 2개에서 7개까지일 때만 기밀 데이터를 삽입한다. 그 이유는 이진 화상의 특성상 연속 길이 L이 $2 \le L \le 7$이라는 것은 해당 블록의 픽셀들의 값들이 0과 1로 대체로 골고루 분포되어 있다는 것이다. 그러므로 해당 블록이 윤곽부분이라는 것을 의미한다. 따라서 기밀 데이터



(a) 4-이웃 픽셀들 (b) 8-이웃 픽셀들

그림 4. 가운데 픽셀과 그 이웃 픽셀들

를 삽입하여도 시각적으로 부담이 가지 않을 것을 예상하여 삽입 블록으로 선택하였다. 또한 연속 길이가 8이라면 이진 카툰 화상의 특성상 그 블록은

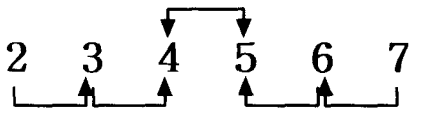


그림 5. 연속 길이 변경 원리

전체 픽셀들이 동일한 픽셀 값을 가질 것이며, 그곳의 픽셀 값 중 한 개를 변경 해버린다면 시각적으로 크게 두드러질 것이기 때문에 제외시킨다. 또한 연속 길이가 1인 경우는 흑백이 번갈아 출현하는 부분으로 기밀 데이터를 추출할 때 오류를 발생시킬 여지가 있어 제외시킨다.

제안 방식 또한 보안을 고려하여 WL 방식과 같이 키 테이블 K를 이용하여 기밀 데이터를 삽입한다. 그러나 제안 방식에서는 키 테이블 생성 방법에서 WL 방식과 차이점을 두었다. 키 테이블 전송을 보다 안전하게 하기 위해 테이블 자체를 공유하는 것이 아니라, seed 값에 의해서 의사난수 코드를 9개를 생성한다. 그리고 식(4) 또는 식(5)와 같이 두 가지 방법으로 삽입할 비트를 생성한다. 즉, 여기서 K는 9개의 의사난수 값이고, b는 기밀 데이터, h_i는 i번째 블록을 의미하고, b'는 삽입할 비트 값이다.

$$b' = K \oplus b \tag{4}$$

$$b' = (h_i \oplus K) \oplus b \tag{5}$$

식(4)와 식(5)를 이용하여 삽입 비트를 생성하는 것은 seed 값을 알지 못하는 제3자에 대해서는 기밀 데이터를 추출할 수 없도록 보안을 고려한 것이다. 제안 방식의 원리를 그림 6에 일예를 들어 나타내었다. 그림 6에서는 8-이웃 픽셀들을 첫 번째인 (1, 1) 픽셀에서부터 주사를 해 나가면 연속적으로 동일한 값을 가지는 픽셀들이 (1, 2)에서부터 (3, 3)까지 발견할 수 있다. 즉, 연속 길이 $L=4$가 되고, 변환지점 $p=(3,2)$가 된다. 그런 다음 L과 삽입 비트 b'를 결합하여 식(6)에 의하여 변환지점 p의 픽셀 값을 변경한다. 단, $L=7$이고 삽입 비트 $b'=0$인 경우와 $L=6$이고 삽입 비트 $b'=1$인 경우는 변환지점을 $p-1$로 해서 변경을 한다.

$$\begin{cases} \text{연속 길이를 짝수화}, & b'=0 \text{ 인 경우} \\ \text{연속 길이를 홀수화}, & b'=1 \text{ 인 경우} \end{cases} \tag{6}$$

앞에서 기술한 제안 방식의 알고리즘으로 수행을 하면 추출할 때 오류가 발생할 경우가 있다. 예를 들면 블록의 8개의 픽셀 값들을 일차원으로 '0 0 0 0 1 0 1 0'인 경우는 $L=4$가 될 것이고, 변환 위치 p는 5번째가 된다. 이 때 삽입 비트 b'가 1인 경우에는 5번째의 값을 0으로 변경해야한다. 따라서 픽셀 값들이 '0 0 0 0 0 0 1 0'으로 변경이 되므로 데이터를 추출할 때 $L=6$이 되므로 추출 데이터는 0으로 오류가 생길 수 있다. 그러므로 제안 방식에서는 이런

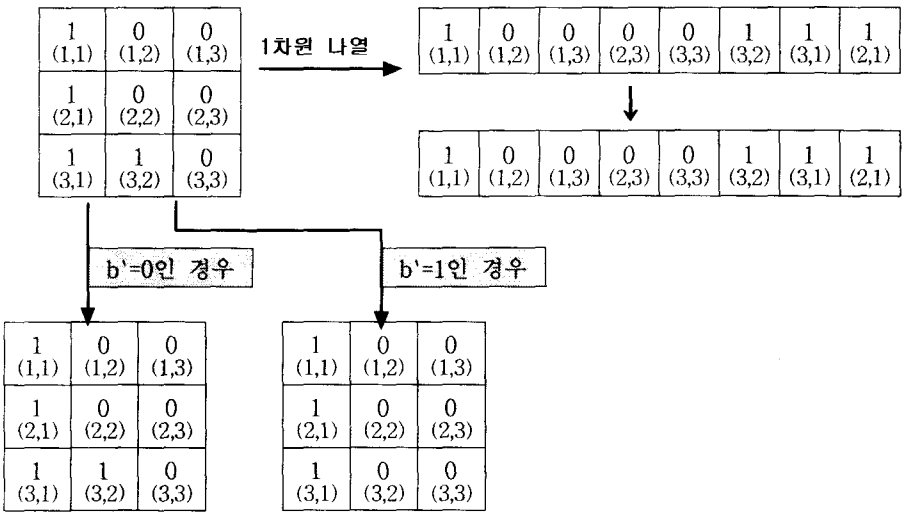


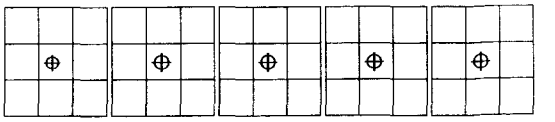
그림 6. 8-이웃 픽셀을 이용한 데이터 삽입

경우에는 p번째의 픽셀 값과 $p+1$째 픽셀 값을 서로 교환하는 방법으로 해결을 하였다. 즉, 위와 같은 경우에는 '0 0 0 0 1 0 1 0'을 '0 0 0 0 0 1 1 0'으로 처리를 하면 추출할 때 오류를 방지할 수 있다.

기밀 데이터의 추출은 삽입에서처럼 화상을 3×3 크기의 블록으로 분할한 후, 블록의 연속 길이 L을 계산한다. 연속 길이가 L이 짝수인지 홀수인지 판단하여, 짝수이면 0을 홀수이면 1을 추출하면 된다.

3.2 가운데 픽셀과 8-이웃 픽셀 적용

본 절에서는 3.1절에 기술한 제안 방식에서 삽입량을 보다 더 증가시키기 위한 개선 방법을 보인다. 삽입 방법은 앞 절에서 기술한 것처럼 8-이웃 픽셀들의 연속 길이를 계산하여 조건에 만족하는 8-이웃에 기밀 데이터 1비트를 삽입한 후, 화상의 경계점인 블록의 가운데 픽셀 값을 조작하여 기밀 데이터를 1비트 추가로 삽입하는 방법이다. 그림 7에서 표현한 것처럼 일반적으로 영상처리에서는 어떤 픽셀을 둘러싼 8개의 이웃 픽셀 중에서 자신과 동일한 색을 갖는 픽셀의 개수 N을 계산하여 $N=0$이면 고립점이라 하고, $N=8$이면 내부점, $1 \le N \le 7$이면 경계점이라 말한다. 따라서 본 개선 방식에서는 경계점을 가지는 블록에 대해서만 가운데 픽셀 값을 변경함으로써 1비트를 추가로 삽입하는 방식이다. 하지만 모든 경계점의 가운데 픽셀 값을 변경하게 되면 화질의 열화가 많이 발생할 것으로 예상되므로 N의 값이 $3 \le N \le 5$의 조건을 만족하는 블록에 대해서 삽입을 하였다.



(a)고립점 (b)내부점 (c)경계점 (N=2) (d)경계점 (N=3) (e)경계점 (N=5)

그림 7. 가운데 픽셀 변경 대상 블록

또한, 개선 방식에서는 삽입 가능한 연속 길이의 값을 $3 \le L \le 7$으로 제한하였다.

개선 방법을 그림 8과 같이 일예를 들어 설명한다. 먼저 크기가 3×12인 호스트 화상 H를 3×3 크기의 블록 B로 분할하면 4개의 블록 B_1, B_2, B_3 그리고 B_4가 생성된다.

여기에 삽입 비트열 '1 0 1 0 0 1'을 삽입한다면, 먼저 첫 번째 블록인 B_1의 연속 길이를 구하면 $L=4$가 되고, 삽입 비트는 '1' 이다. 그러므로 연속 길이를 홀수로 변경해야 한다. 이때 변환 위치 p는 (3, 1)이므로 블록 B_1의 (3, 1)의 픽셀 값을 '1'로 변경한다. 또한 변경 후 삽입하고자 하는 비트 값과

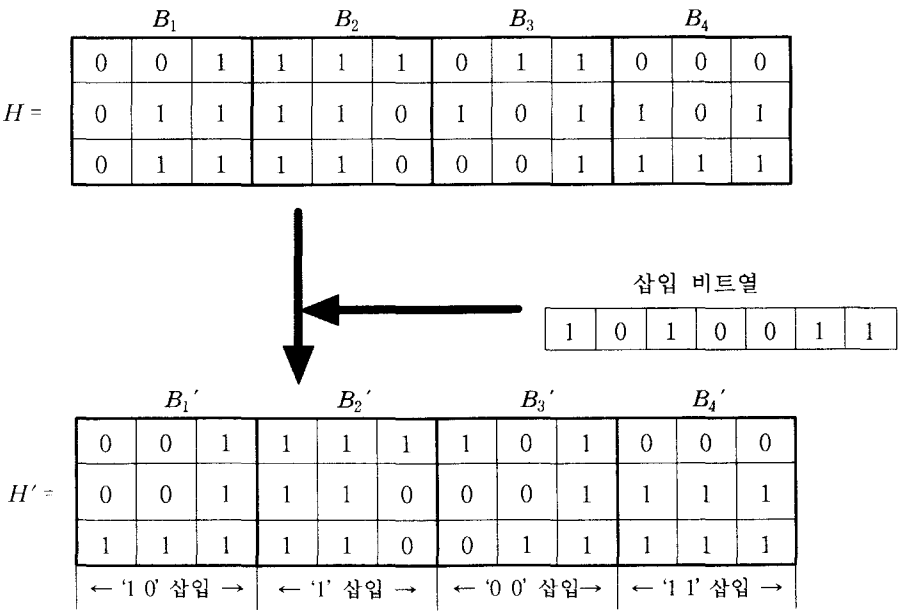


그림 8. 가운데 픽셀과 8-이웃 픽셀을 이용한 삽입 방법

8-이웃 픽셀 값들과의 동일한 값이 몇 개인지 비교하여 N을 계산한다. 블록 B_1은 $N=3$이 되므로 가운데 픽셀에 1비트를 추가로 삽입을 할 수 있다. 따라서 두 번째 비트인 '0'을 가운데 픽셀에 삽입을 한다. 그러므로 첫 번째 블록 B_1에는 2비트를 삽입할 수 있게 된다. 그러나 두 번째 블록인 B_2에서는 $L=3$이고, 삽입 비트는 '1'이며 변환 위치 p는 (2, 3)이 된다. 하지만 연속 길이가 홀수인 3이므로 변환을 할 필요가 없으며, 또한 삽입 후 다음 삽입 비트의 값과 8-이웃 픽셀 값과의 동일한 픽셀 개수가 몇 개인지 계산하면 $N=2$이 된다. 따라서 가운데 픽셀에 1비트를 추가로 삽입할 수 없기 때문이 블록 B_2에는 1비트만 삽입한다. 같은 방법으로 블록 B_3에는 $L=4$, $N=3$으로 2비트 '0 0'이 삽입되고, 블록 B_4에는 $L=3$, $N=5$가 되므로 '1 1'의 2 비트가 삽입이 된다.

기밀 데이터를 추출할 때에는 앞 절의 제안 방식처럼 블록의 연속 길이 L을 계산한 후, 그 수가 짝수인지 홀수인지를 판단한다. 만약 연속 길이 L이 짝수이면 0을, 홀수이면 1을 추출하면 된다. 또한 해당 블록의 패턴이 가운데 픽셀 값과 동일한 픽셀 값이 몇 개인지 계산하여 $3 \le N \le 5$인 블록에서는 가운데 픽셀 값을 추가로 1비트 더 추출하면 된다. 이처럼 추출한 데이터는 기밀 데이터가 아니므로 seed 값을 이용하여 삽입과정에서 수행한 것 같이 의사난수 코드 9개를 생성하여 식(4) 또는 식(5)를 이용하여 역으로 계산하면 기밀 데이터를 추출할 수 있다.

4. 실험 결과 및 고찰

기존의 방식들과 제안 방식의 성능을 비교하기 위하여 실험을 하였다. 실험 대상 화상은 흑/백의 두 값으로 구성된 이진 카툰 화상 Lucy(150×270)와 Snoopy(240×360)를 대상으로 하였으며, 기밀 데이터는 문자열 비트(0 또는 1)를 삽입에 이용하였다. 추출은 공격을 배제한 상태이므로 완벽하게 전체 기밀 데이터를 추출할 수 있었다.

기존의 방식들과 제안 방식에 대해서 표 1 및 표 2와 같은 결과를 얻을 수 있었다. 여기서 삽입량은 호스트 화상에 삽입된 기밀 데이터의 비트 수이며, 차분은 원 화상과 기밀 데이터를 삽입한 화상간의 상이한 픽셀의 개수이다. 또한 식(6)과 같이 NC를 이용하여 평가하였다. 식(6)에서 W는 원 화상, W_r는 기밀 데이터 삽입 화상을 의미한다.

$$NC = \frac{\sum_i \sum_j W(i,j) \cdot W_r(i,j)}{\sum_i \sum_j [W(i,j)]^2} \tag{6}$$

표 1. 기존방식과 제안 방식의 비교-I (단위 : 픽셀 개수)

구분		WL 방식	PWW 방식	제안 방식	개선방식 ($3 \le N \le 7$)
삽입량	Lucy	805	532	1,053	1,633
	Snoopy	1,112	649	1,606	2,377
차분	Lucy	680	246	647	821
	Snoopy	948	325	940	1,288

표 2. 기존방식과 제안 방식의 비교-II (단위 : %)

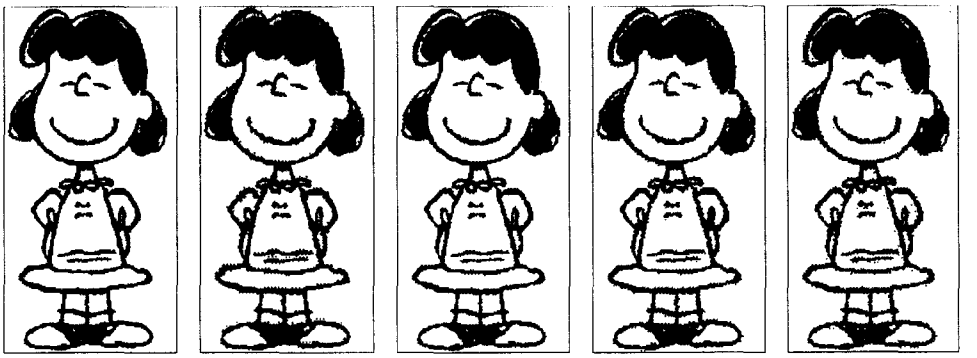
구분		WL 방식	PWW 방식	제안 방식	개선방식 ($3 \le N \le 7$)
삽입량 / 전체크기	Lucy	1.99	1.31	2.60	4.03
	Snoopy	1.29	0.75	1.86	2.75
차분 / 삽입량	Lucy	84.47	46.24	61.44	50.28
	Snoopy	85.25	50.07	58.53	54.19
NC	Lucy	0.982	0.998	0.990	0.989
	Snoopy	0.999	0.999	0.993	0.993

그림 9와 그림 10에서는 원 화상과 WL 방식, PWW 방식 그리고 제안 방식 및 개선 방식을 실험한 결과 화상들이다.

표 1, 2 및 실험 화상(그림 9, 10)을 보면 알 수 있듯이, WL 방식은 화상의 윤곽 부분 주위에 잡음들이 모여 있으며, 삽입량 또한 제안 방식에 비해서 적음을 알 수 있다. 표 1, 2에서 L은 연속 길이를 의미한다. 또한 PWW 방식에서 원 화상과의 차분이 WL 방식과 제안 방식에 비해 작은 것은 삽입량이 제안 방식의 절반에 미치지 못하기 때문이다. 또한 제안 방식은 데이터의 삽입량에 따라 연속 길이에 제한을 두어 삽입 블록을 선택할 수 있으므로 화상에 따라 적응적으로 사용할 수 있다는 장점이 있다. 삽입량, 차분, 화질 등을 기존의 방식들과 비교해 볼 때 본 제안 방식이 더욱 우수함을 확인할 수 있다.

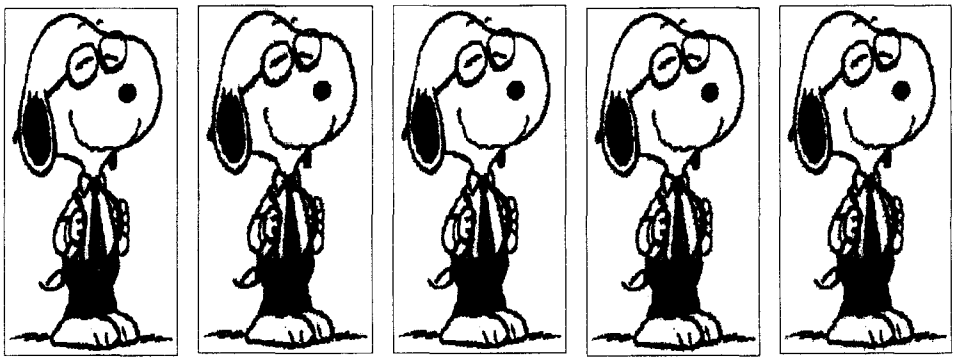
5. 결론 및 향후 과제

본 논문에서는 이진 카툰 화상을 이용하여 기밀



(a) 원 화상 (b) WL 방식 (c) PWW 방식 (d) 제안 방식 (e) 개선 방식 ($3 \le N \le 7$)

그림 9. 원 화상(Lucy)과 삽입 화상들



(a) 원 화상 (b) WL 방식 (c) PWW 방식 (d) 제안 방식 (e) 개선 방식 ($3 \le N \le 7$)

그림 10. 원 화상(Snoopy)과 삽입 화상들

데이터를 삽입하는 스테가노그라피의 한 방법을 제안하였다. 제안 방식은 화상을 블록 단위로 분할하고, 블록의 가운데 픽셀을 기준으로 8-이웃 픽셀들의 동일한 연속 길이 값들을 이용하여 데이터를 삽입하였다. 또한, 삽입량의 개선을 위해 경계점에 해당하는 블록에 대해서는 가운데 픽셀의 값도 조작하여 경우에 따라서 한 블록 내에 2비트를 삽입시킬 수 있다. 제안 방식은 시각적으로나 데이터 삽입량의 측면에서 기존 방식에 비해 우수함을 알 수 있었다.

향후 과제로 이진 카툰 화상의 특징을 이용하여 더욱 많은 기밀 데이터를 시각적으로 영향을 주지 않으면서 삽입하도록 개선하는 것이다. 또한 이러한 연구를 기반으로 다치 카툰 화상 및 컬러 화상에 적용할 수 있도록 하는 것이다.

참 고 문 헌

[1] 박영란, 이혜주, 박지환 "오차 확산법을 이용한 기밀 데이터 합성법", 한국멀티미디어학회 논문지, 제2권 2호 p.155-165, 1999. 6.

[2] Yasushi Abe Koichi Inoue, Koichi Ejiri "Digital Watermarking for Bi-Level Image", Proc. of Symposium on Crypotography and Information Security 2000, C05, 2000. 1.

[3] M.Y. Wu, J.H. Lee "A Novel Data Embedding Method for Two-Color Facsimile Images." In Proc. of International Symposium on Multimedia Information Processing(ISMIP98), 1998. 12.

[4] Gang Pan, Yijun Wu, Zhaohui Wu, "A Novel Data Hiding Method for Two-Color Image", International Conference on Information and Communications Security(ICICS2001), LNCS 2229, p.261-270, 2001

[5] Hsiang-Kuang Pan, Yu-Yuan Chen, Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Image", Proc. IEEE Symposium on Computer and Communication(ISCC 2000), p.750-755, July 2000.

[6] Gang Pan, Zhaohui Wu, Yunhe Pan "A Data Hiding Method for Few-Color Images", IEEE International Conference on Acoustics, Speech, and Signal Processing(ICASSP'02), Vol.4, p.3469-3472, May 2002.

[7] Min Wu, Edward Tang, Bede Liu, "Data Hiding in Digital Binary Image", IEEE Int. Conf. on Multimedia and Expo(ICME 2000), p.393-396, July 2000.

[8] C.-C. Chang, M.-N. Wu, K.-F. Hwang, "High Quality Perceptual Data Hiding Technique for Two-Color Images", Proceedings of Pacific Rim Workshop on Digital Steganography 2002, p.65-70, July 2002.

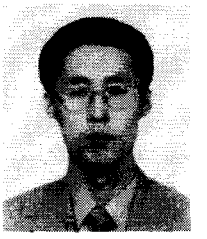
[9] Yu-Chee Tseng, Hsiang-Kuang Pan, "Secure and Invisible Data Hiding in 2-Color Images", Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001), Vol.2, p.887-896, April 2001.

[10] Kuo-Feng Hwang, Chin-Chen Chang, "A Run-Length Mechanism for Hiding Data into Binary Images", Proceedings of Pacific Rim Workshop on Digital Steganography 2002, p.71-74, July 2002.

박 영 란

1996년 2월 방송통신대학 전자계산학과 졸업(이학사)
1998년 8월 부경대학교 전산정보학과 졸업(이학석사)
2003년 3월 ~ 현재 부경대학교 정보보호학과 박사과정

관심분야 : 심층암호, 워터마킹, 영상처리



박 지 환

1990년 3월 일본 요코하마국립대 전자정보공학 졸업(공학박사)
1994년 9월 ~ 1995년 3월 동경대 생산기술연구소 방문 연구
1998년 1월 ~ 1998년 2월 전기통신대학(일본), 방문연구
1999년 7월 ~ 1999년 8월 Monash University, Australia, Visiting Research
2001년 2월 ~ 2001년 3월 Communication Research Lab
1992년 (CRL) Japan, STA Fellowship
1996년 4월 ~ 현재 동경대학 생산기술연구소 협력연구원
1990년 3월 ~ 현재 부경대 컴퓨터멀티미디어공학부 교수
1997년 3월 ~ 현재 한국정보보호학회 이사
2002년 3월 ~ 현재 한국정보보호학회 영남지부장
1998년 12월 ~ 현재 한국멀티미디어학회 운영위원 논문지 편집위원
1999년 3월 ~ 현재 한국정보처리학회 논문지 편집위원
2002년 3월 ~ 현재 한국정보보호학회 논문지 편집위원
2002년 1월 ~ 2월 CRL 방문연구 JSPS Fellowship
관심분야 : 멀티미디어 컨텐츠 보호 및 응용, 암호학